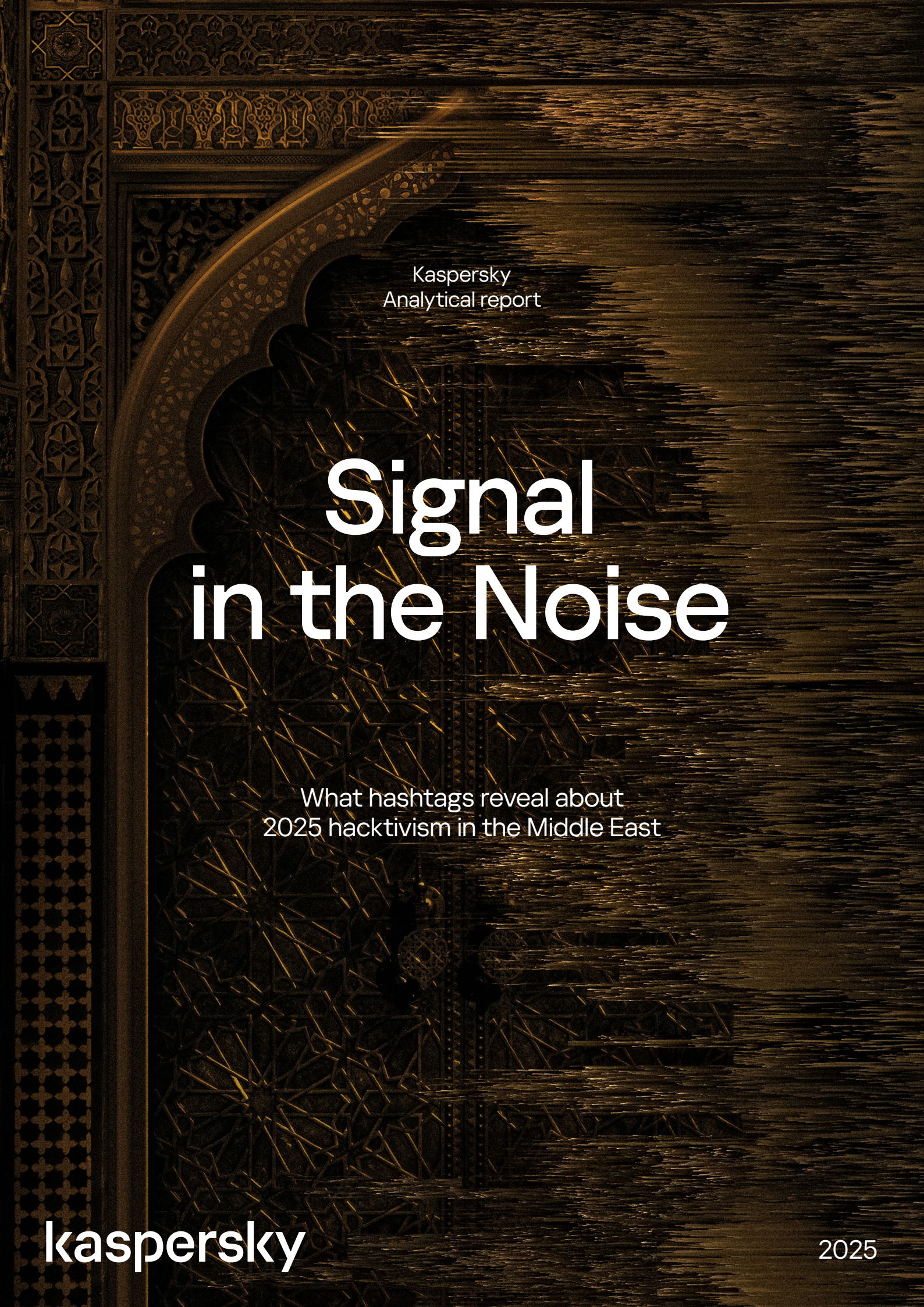


Kaspersky
Analytical report

Signal in the Noise

What hashtags reveal about
2025 hacktivism in the Middle East

kaspersky

2025

Signal in the noise: What hashtags reveal about 2025 hacktivism

Executive summary

This study analyzes more than 11,000 hacktivist posts across surface and dark web sources and finds that most planning and mobilization happens in the open[1].

The targeting is global, extending well beyond MENA into Europe, the Americas and Asia. Hashtags are the connective tissue of these operations, used as group identifiers, campaign tags and claims of responsibility; they are posted constantly for coordination and visibility rather than stealth.

Hashtags also map alliances and momentum. We identify 2,063 unique tags in 2025 — 1,484 appearing for the first time, and many tied directly to specific groups or joint campaigns. Most tags are short-lived (about two months), with "popular" ones persisting longer when amplified by alliances; channel bans contribute to attrition.

Operationally, reports of completed attacks dominate hashtagged content (58%), and within those, DDoS is the workhorse (61%).

Spikes in threatening rhetoric do not by themselves predict more attacks, but timing matters: when threats are published, they typically refer to actions in the near term, i.e. the same week or month, making early warning from open-channel monitoring materially useful.

For defenders and corporate leaders, the implications are direct: Prioritize scalable DDoS mitigation and proactive security measures, and treat public threats as short-horizon indicators rather than long-range forecasts. Invest in continuous monitoring across Telegram and related ecosystems to surface alliance announcements, threat posts and cross-posted "proof" rapidly. And even organizations outside conflict zones should assume exposure: hacktivist campaigns seek reach and spectacle, not narrow geography, and hashtags remain a practical lens for separating noise from signals that demand action.

1 This study draws upon content produced by more than 120 hacktivist groups engaged in the Middle Eastern conflict. Entities identified as supporting Israel exhibited minimal activity; consequently, the findings primarily reflect the output of groups publicly associated with the Arab world. The analysis is undertaken exclusively from a cyber perspective and is anchored in the principle of neutrality.

Introduction

What do hacktivist campaigns look like in 2025?

This research provides the answers based on analysis of posts circulating across both the surface web and the dark web, with a particular focus on groups targeting MENA countries.

While it may be assumed that most operations unfold on hidden forums, the reality is different: the most action happens in plain sight. Telegram has become the command center for today's hacktivist groups, hosting the highest density of attack planning and calls to action.

The goal of this report is to highlight patterns in hacktivist operations — including attack methods, public warnings and stated intent. Hacktivists are politically motivated threat actors who typically value visibility over sophistication. Their tactics are designed for maximum visibility, reach and ease of execution, rather than stealth or technical complexity. A 'hacktivist' may refer to either the administrator of a community who initiates the attack, or to an ordinary subscriber who simply participates in the campaign.

They're loud. They're flashy. And they want to be seen

One notable feature of hacktivist posts and messages on dark web resources is the frequent usage of hashtags (#word/s). Used in their posts constantly, hashtags often serve as political slogans — amplifying messages, coordinating activity or claiming credit for attacks. The most common themes are political statements and hacktivist groups names, though hashtags sometimes reference geographical locations such as specific countries or cities.

In total, we analyzed more than 11,000 posts containing hashtags — nearly 20% of all hacktivist content we traced across channels from over 120 groups in 2025. Our analysis revealed:

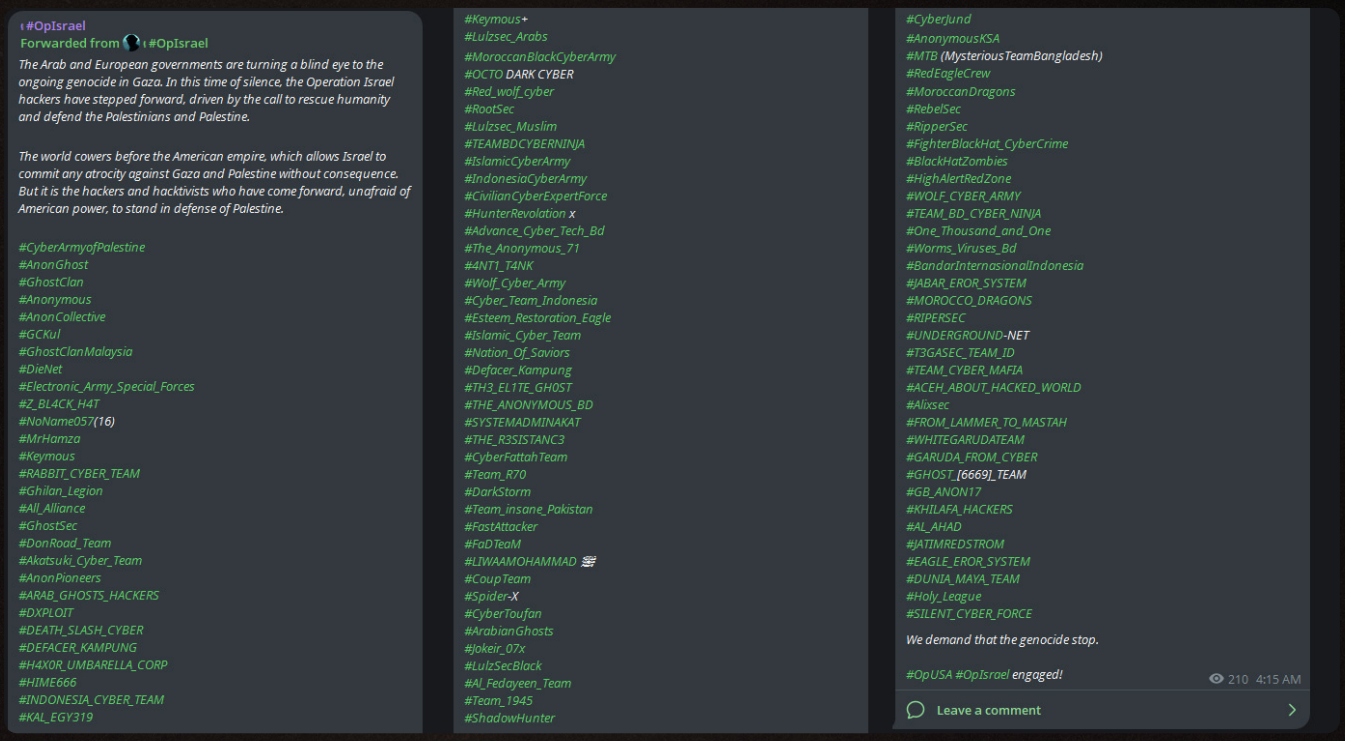
How hashtags are used to coordinate attacks or claim credit

The types of cyberattacks being promoted or celebrated

Patterns across campaigns and regions

How long it typically takes for attack to be reported after the initial threat post

Fig. 1 | Motivation behind OpIsrael group



Let's take a look at some examples of popular hashtags in 2025:

#nation_of_saviors

Refers to a hacktivist group that first appeared in January 2025 and has maintained visibility throughout the year. Among mentioned victims there are entities across India, Israel, Germany, United Kingdom, Vietnam, Indonesia, and other counties.

#globalfront

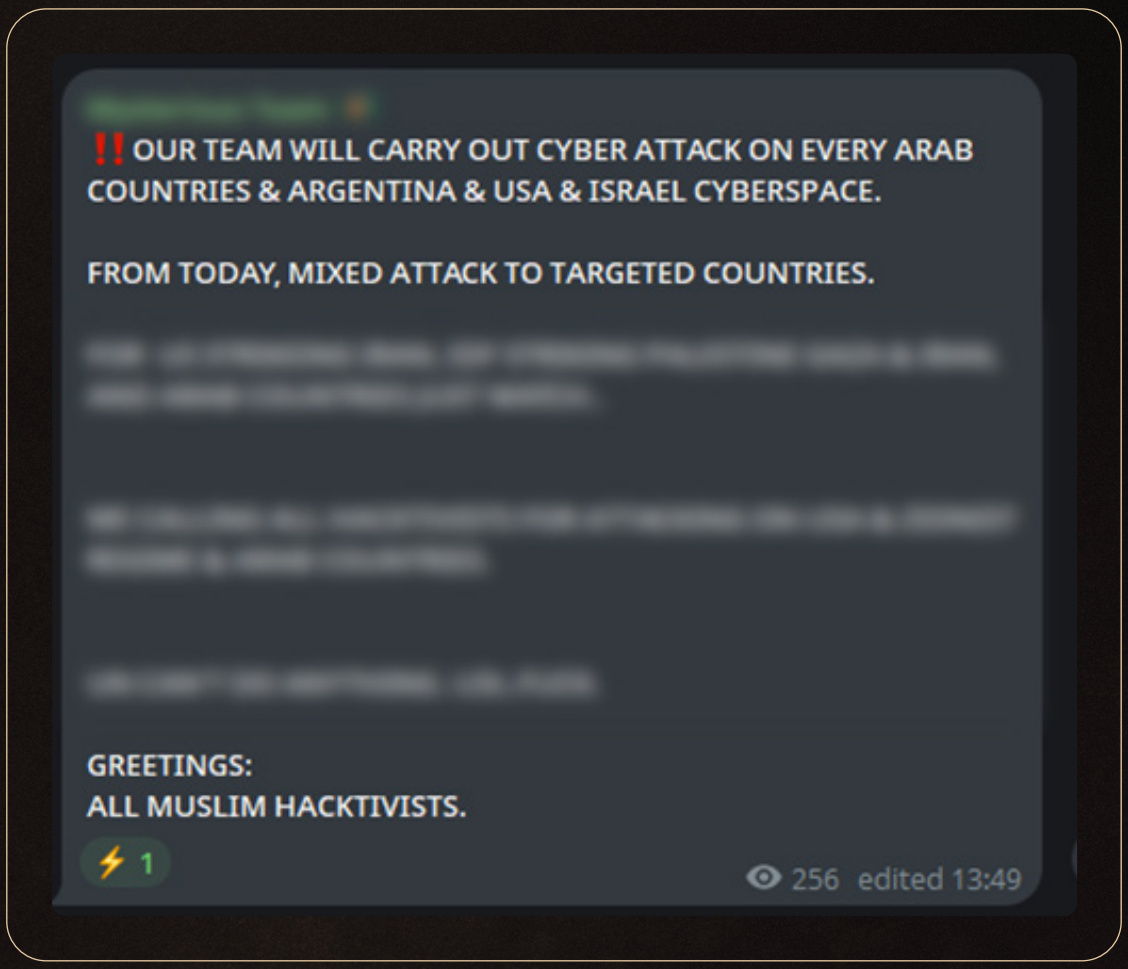
Associated with a targeted campaign by the group **Arabian Ghosts**, active from April to June 2025. The hashtag was used to coordinate and report on a wave of cyberattacks on Middle East, as well as India and USA government organizations during this period.

#vulture

Originally connected to an eponymous group that emerged in February 2025 but has since gone inactive. The hashtag, however, continues to be used in alliance-related messages.

Hacktivist operations in 2025 are no longer limited to actors directly involved in armed conflicts. Instead, they are casting their net deep and wide globally, targeting a wide range of regions. There are victims throughout Europe and Middle East, as well as Argentina, the United States, Indonesia, India, Vietnam, Thailand, Cambodia, Türkiye, and others.

Fig. 2 | Motivation behind attacks by Mysterious Team

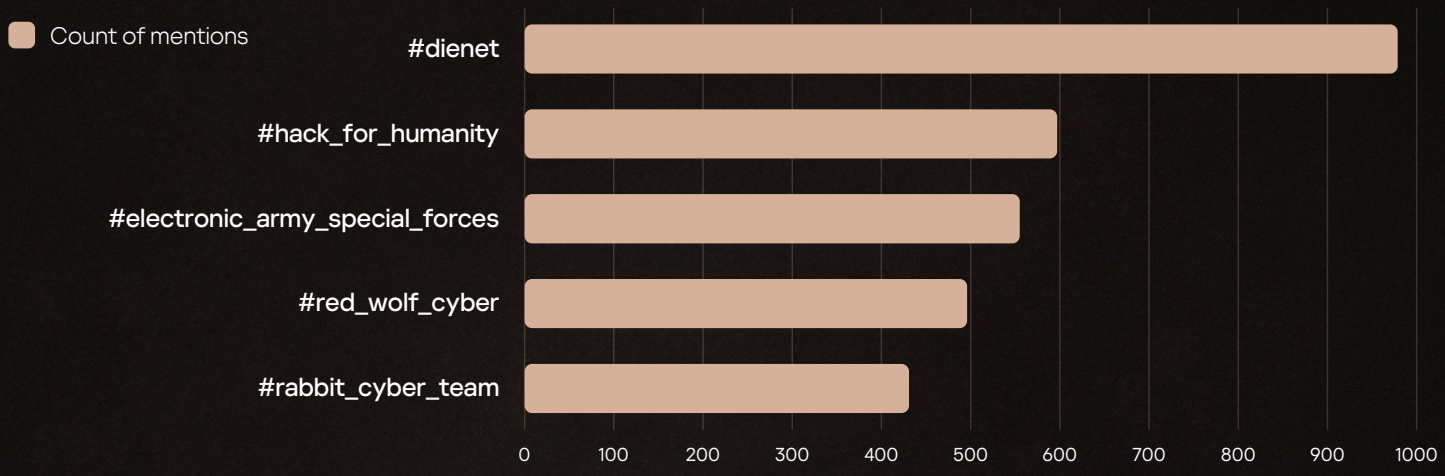


Hacktivist activity in 2025

We identified 2,063 unique hashtags used in hacktivist publications so far in 2025. 1,484 of these are new, with their first appearance this year.

Taking a closer look to the top 5 emerging hashtags so far this year, we discovered that four of them are directly tied to the names of specific hacktivist groups, while the fifth is associated with a joint campaign coordinated by an alliance of several groups.

Fig. 3 | Top 5 new hashtags in 2025



#dienet

Refers to the hacktivist group **DieNet.** First appeared in March 2025 and continues to trend. Commonly used by the group itself and by **Anonymous** in the reports on attacks on wide range of countries: Israel, Vietnam, Cambodia, Canada, USA, Cyprus, ant other.

#hack_for_humanity

Coordinated campaign run by the alliance of **Keymous+, Mr Hamza, Alixsec** and **NoName057.** First seen in February 2025, and remains in use across multiple platforms in messages reporting attacks on Middle East and Europe.

#electronic_army_special_forces

Represents a hacktivist group first mentioned in March 2025, which remains active and operational. Recent targets include Israeli, Chinese, and Cambodian entities.

#red_wolf_cyber

Associated with a group that debuted in February 2025. The group is still active, with a regular presence in Telegram posts regarding DDoS attacks performed on Israel, Cambodia, and Vietnam.

#rabbit_cyber_team

Originally the name of a group that has since disbanded. Despite its inactivity, the hashtag continues to appear in post by the group's allies.

Hacktivist alliances

Humans are social creatures with no exceptions to hacktivists.

Like other social groups, hacktivists frequently form alliances. These collaborations are often announced on hacktivist channels, with bold language, heavy use of symbolism and, of course, hashtags. Based on groups' own statements and our observations, alliances are typically formed to achieve the following strategic goals:

Pooling resources to enable larger and more sustained attacks

Intimidating targets through greater scale and visibility

Increasing overall operational impact

Enhancing reputation and credibility within the hacktivist community

Messages about alliances usually include hashtags from the participating groups, reinforcing mutual recognition and visibility. In some cases, entirely new hashtags are created to represent the alliance.

One example is the public declaration of partnership between Team Fearless and Ghillan Legion.

Fig. 4 | Example of a message publicizing an alliance

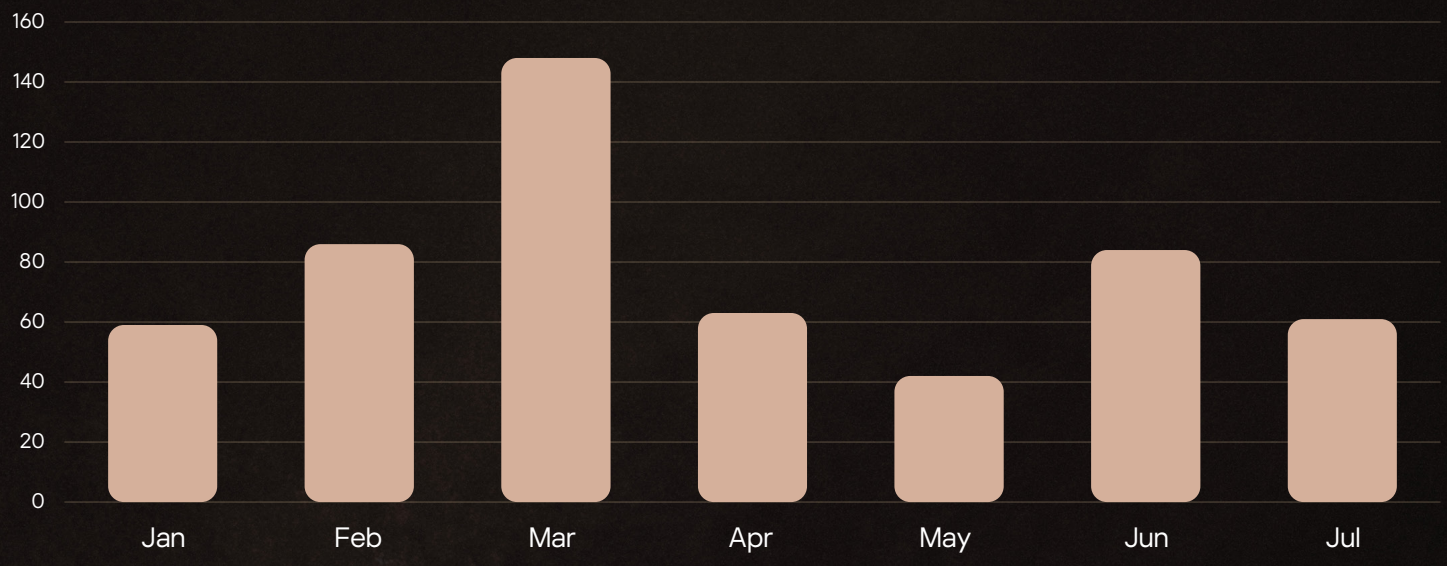
Alliance-related hashtags most commonly appear in:

Hacktivist statements (manifestos outlining their motivations)

Attack reports (summaries of impact, often accompanied by proof of the attack)

This type of hashtag placement makes it easier to track cross-group activity and collaboration.

Fig. 5 | Distribution by month of messages regarding alliance creation, 2025

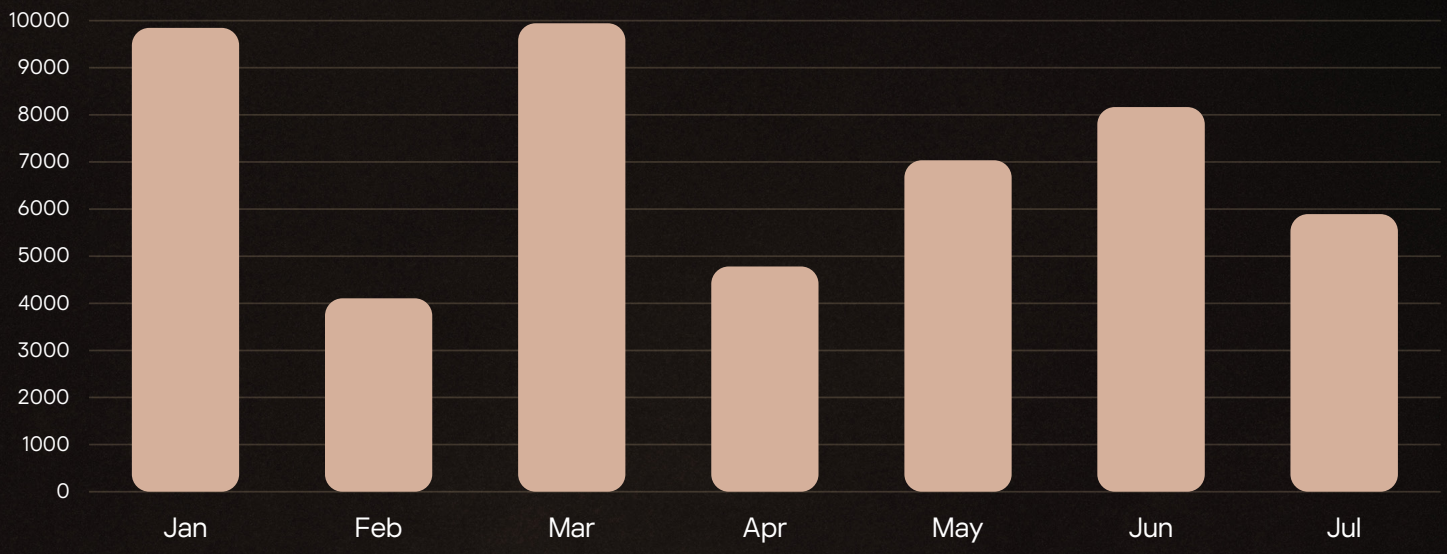


Statements and attack reports are often reposted within the alliance, with each post appearing an average of twice.

Hashtag trends

The rise and fall of hacktivist activity is often closely related to world events. When tensions escalate or new conflicts arise, hacktivists react quickly by launching new campaigns, forming alliances, and posting threatening messages.

Fig. 6 | Monthly distribution of hashtags, 2025



Where hacktivists post

Telegram is the primary communication hub for hacktivist operations. It's the main platform for launching campaigns, publishing statements and sharing reports of conducted attacks.

Our analysis of outbound links in hacktivist posts with hashtags confirms Telegram's dominance:

88%
of references point to Telegram

10%
point to Twitter (X)

The remaining **2%**
are spread across other social media platforms

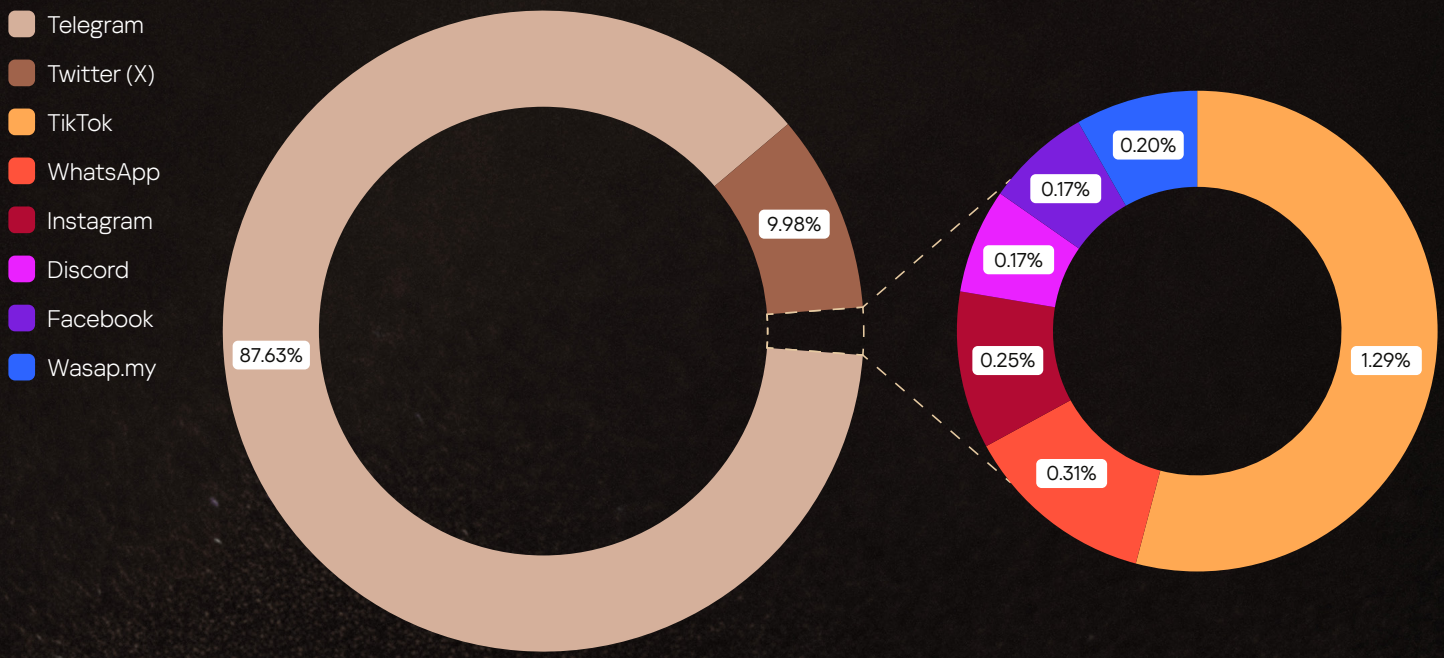
Within this 2% of external links:

Some proudly reference news articles that mention the group

A few link to compromised social media accounts

Others point to additional communication channels or resources run by the same group

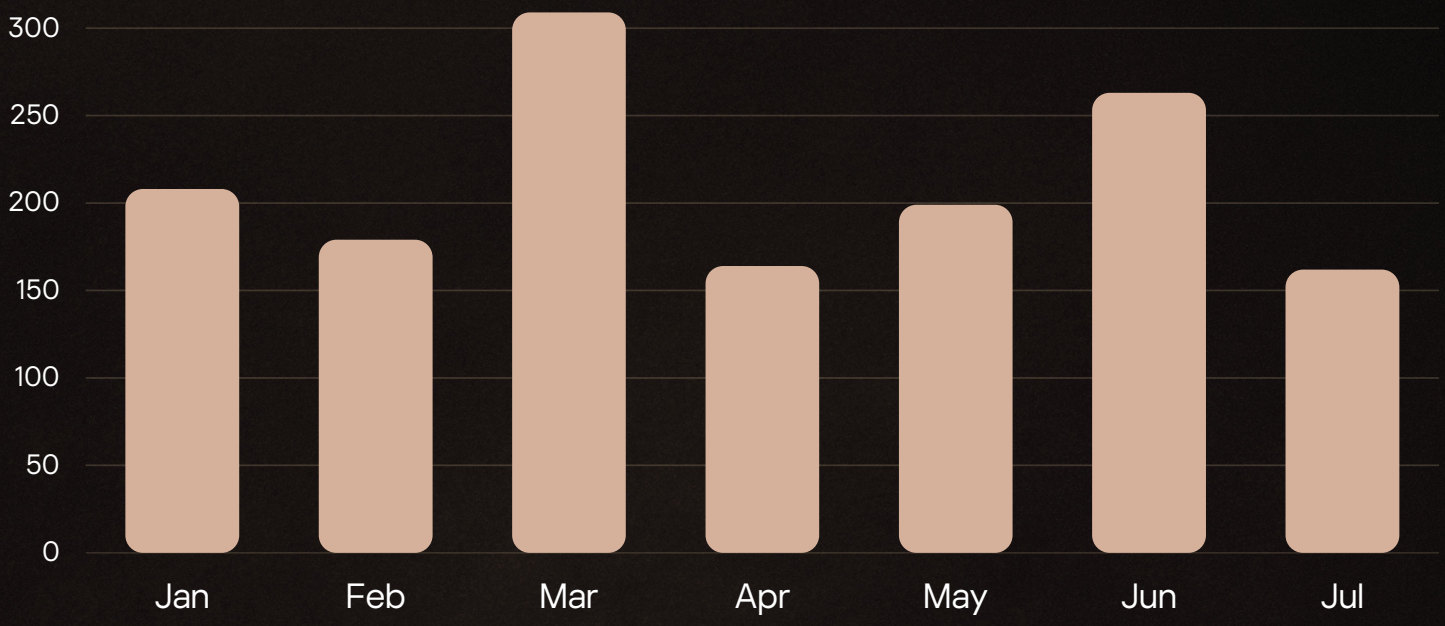
Fig. 7 | Distribution of social media references in posts published in 2025



Hashtag lifetime

220 new hashtags appeared every month in 2025

Fig. 8 | Distribution of new hashtags in 2025

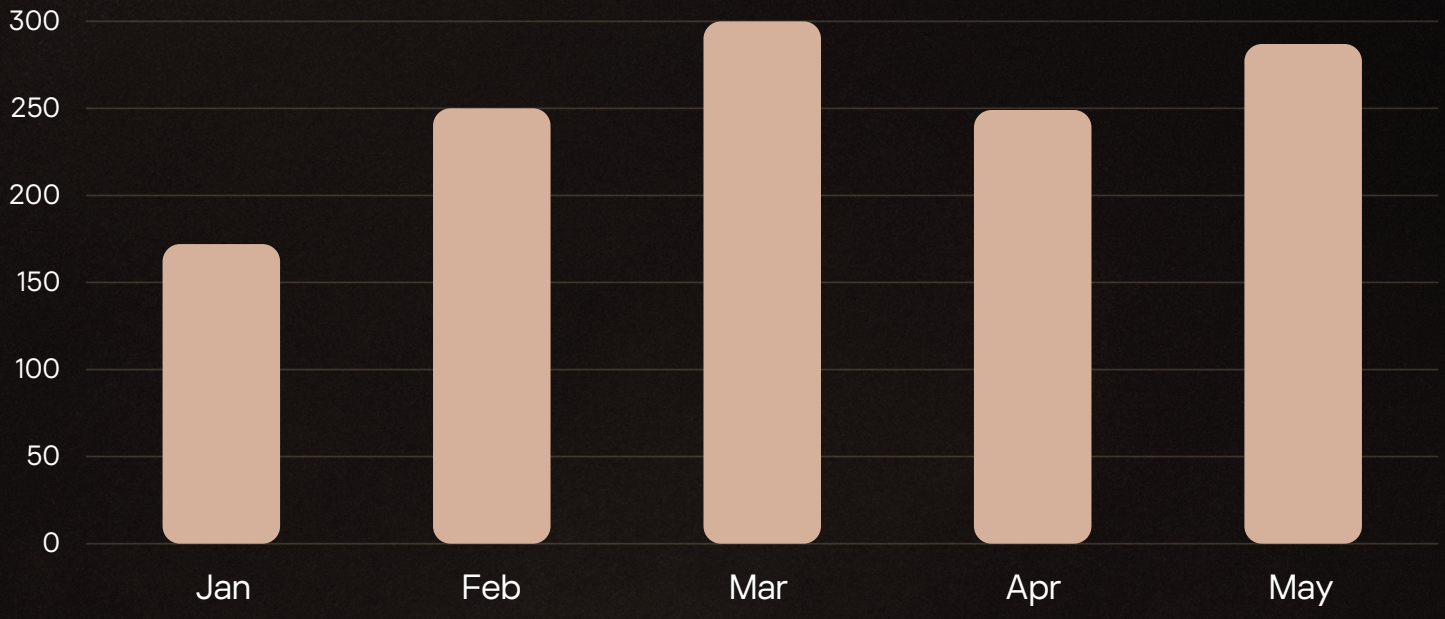


On average, a hashtag lasted 2 months within the past 15 months.

Hacktivist Telegram channels are often banned. While some are resurrected, many hashtags disappear permanently when their original channels are shut down.

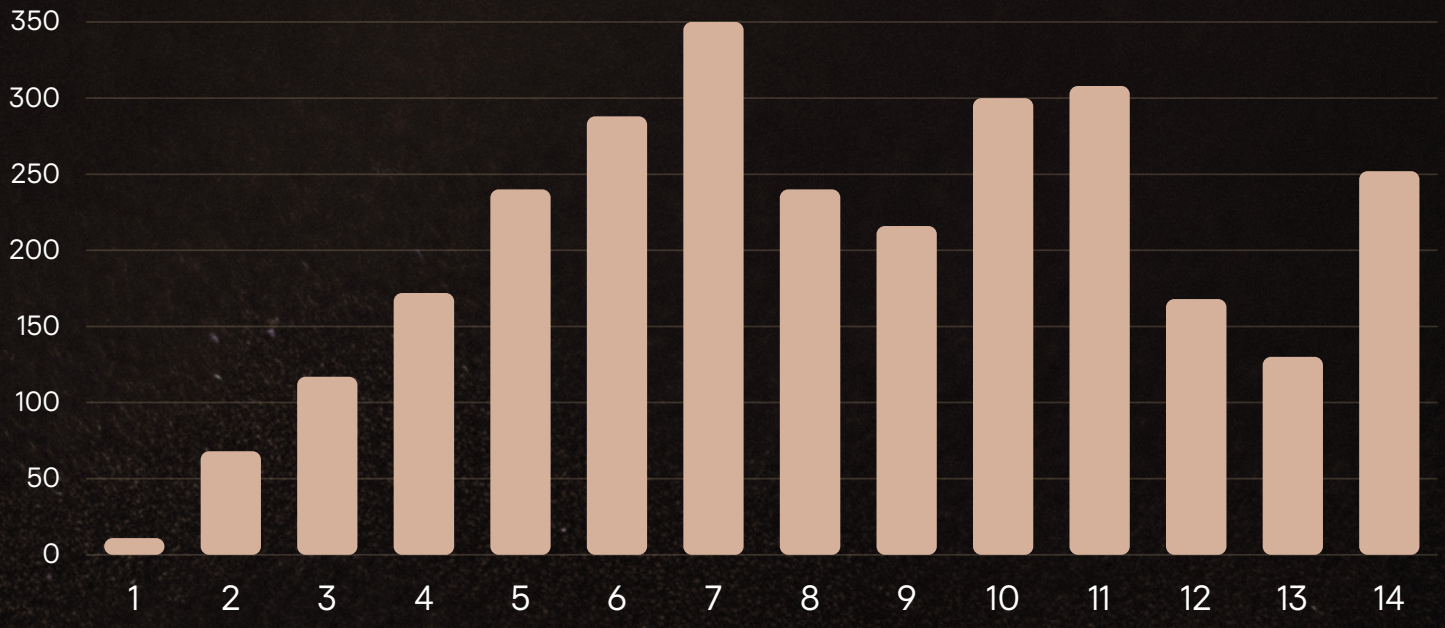
250 hashtags “died”[2] every month in 2025.

Fig. 9 | Distribution of hashtags that ‘died’ in 2025



Popular[3] hashtags lasted significantly longer, with an average lifetime of 6.7 months.

Fig. 10 | Distribution of popular hashtag lifetimes (by count in month)



2 A hashtag is considered “dead” if it has not been used for more than two months. Based on this definition, the most recent available data on inactive hashtags is from May 2025 onwards.

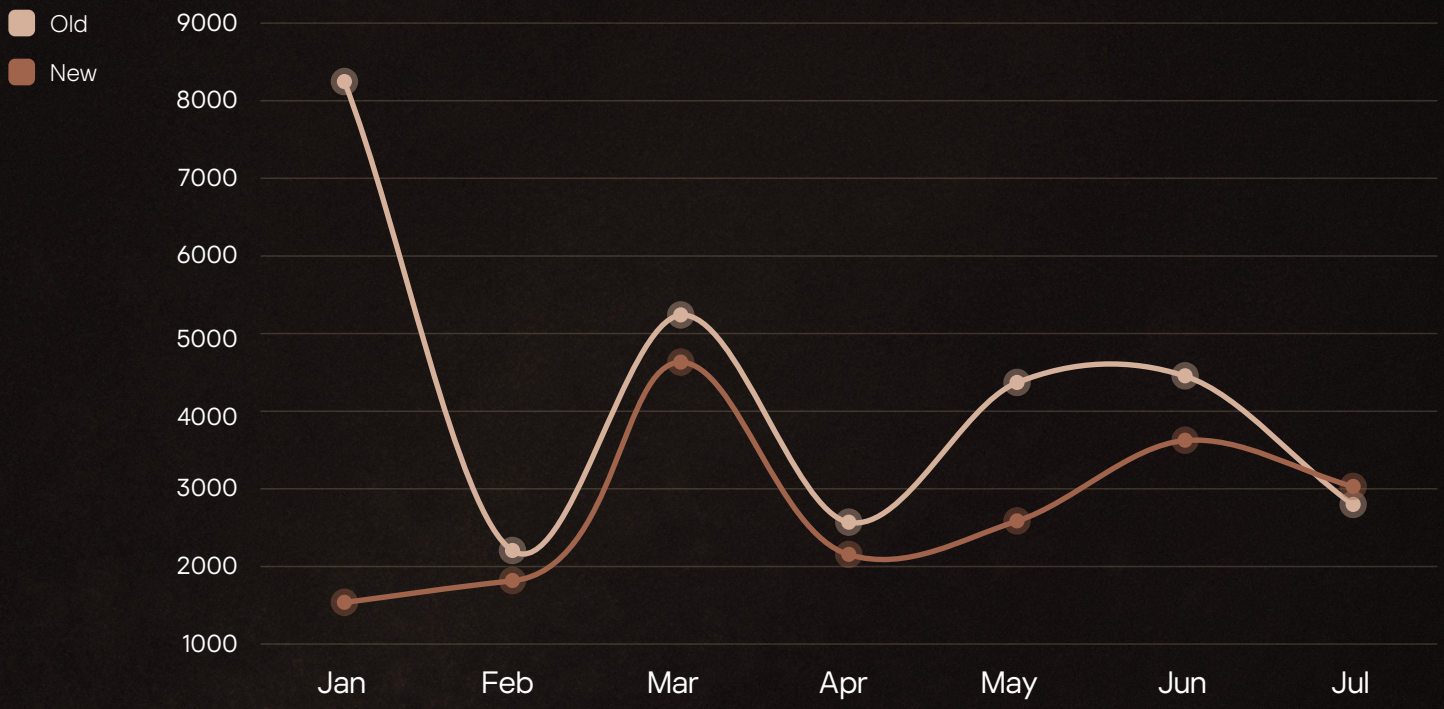
3 A hashtag is considered “popular” once it has been mentioned at least 100 times within past 15 months.

Activity patterns

In March and April 2025, 73% of popular older hashtags (created before 2025) fell silent.

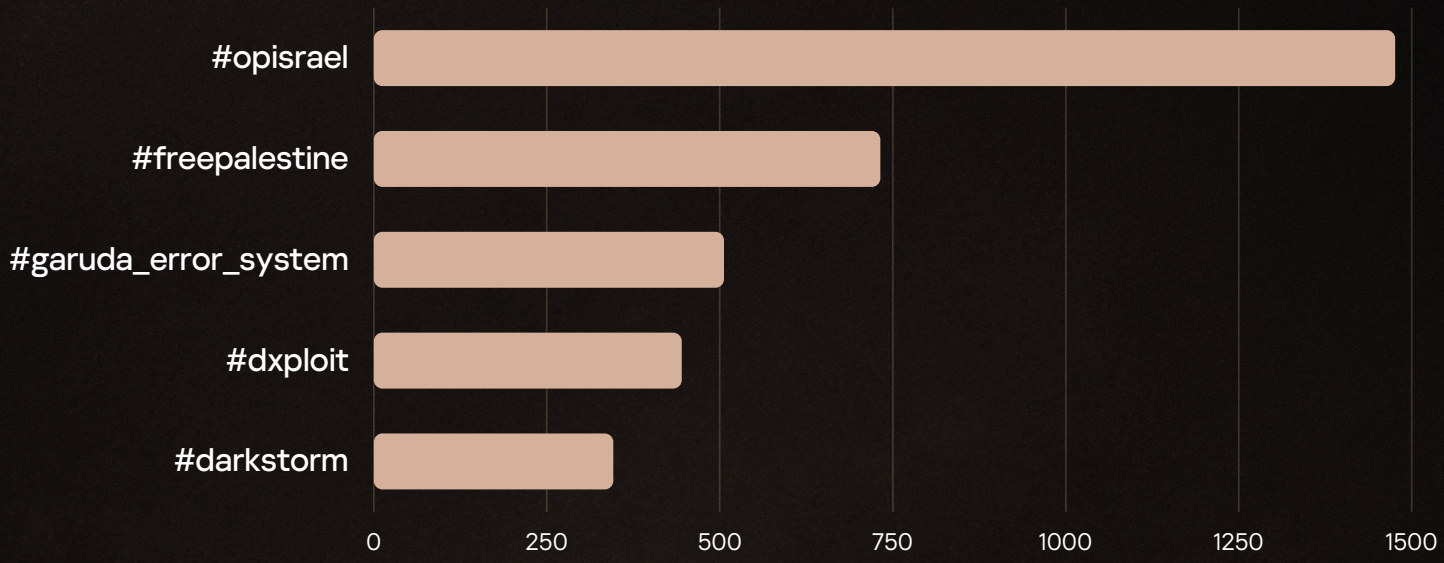
They reappeared in May, following the return of the RipperSec hacktivist group, which brought back both its own hashtag along with those of its allies. This spike in activity was not observed among newer hashtags created in 2025. In July, older hashtags fell silent again, while new hashtags became more widely used than old ones for the first time.

Fig. 11 | Mentions of old and new hashtags in 2025



The figure below shows the five oldest hashtags by number of mentions in 2025 — each has remained active for at least 15 months. In total, 18 hashtags have shown this kind of long-term activity.

Fig. 12 | Top 5 oldest hashtags by the number of mentions in 2025



#opisrael

Both the name of a hacktivist group and a political statement. One of the most popular and widely used hashtags. Uniquely, it is actively used by channel administrators and subscribers.

#freepalestine

A well-known political slogan, originally spread through mainstream social media. Appears in 10% of all messages containing hashtags.

#garuda_error_system

Hacktivist group name. Active since 2024, and still highly active. Frequent reposting within alliances makes it the most used group hashtag among the older ones. Israel, India, Nepal, and Cambodia are among the most targeted countries.

#dxploit

Hacktivist group name. Active since 2024, but gradually losing visibility, with mentions decreasing throughout 2025. European and Israeli websites are among the most mentioned targets of attacks.

#darkstorm

Hacktivist group name. Active since 2023. Rarely joins alliances, resulting in one of the lowest repost rates, but continues to publish a high volume of original content regarding attacks on Syria, Israel, Iran, Thailand, Lebanon, Egypt, and multiple European entities.

Message context and categories

We analyzed over 11,000 hacktivist posts containing hashtags and classified them into the following categories:

Reports on completed attacks:

- DDoS
- Defacement
- Data breach
- Doxing
- Credential leaks / access disclosures
- Network infrastructure reveals
- Uncategorized attacks

Upcoming attack warnings —

announcements of planned attacks on specific companies or countries

Hacktivist statements —

explanations on the motivation behind their ideology and their targets

Alliance formation —

announcements of planned attacks on specific companies or countries

Promotion —

invitations to join new Telegram channels (often after bans) or advertisements for services such as hosting or proxies

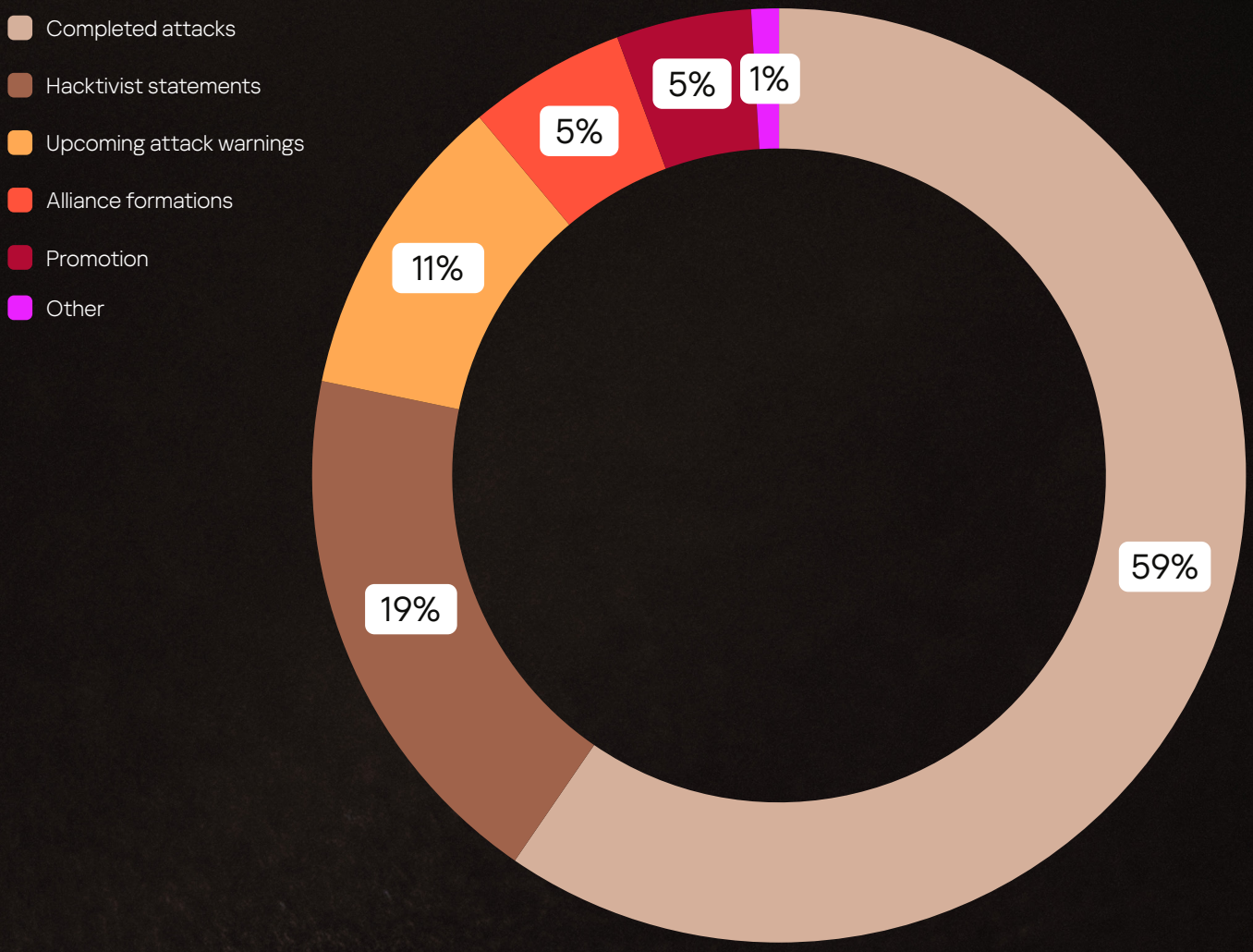
Other:

- **News** — about global events or public mentions about a group
- **Recruitment** — calls to join hacktivist teams
- **Attack summaries** — periodic operational reports
- **Guides and tutorials** — guides and tutorials on how to organize DDoS, penetration testing, and related tactics

Dominance of DDoS attacks

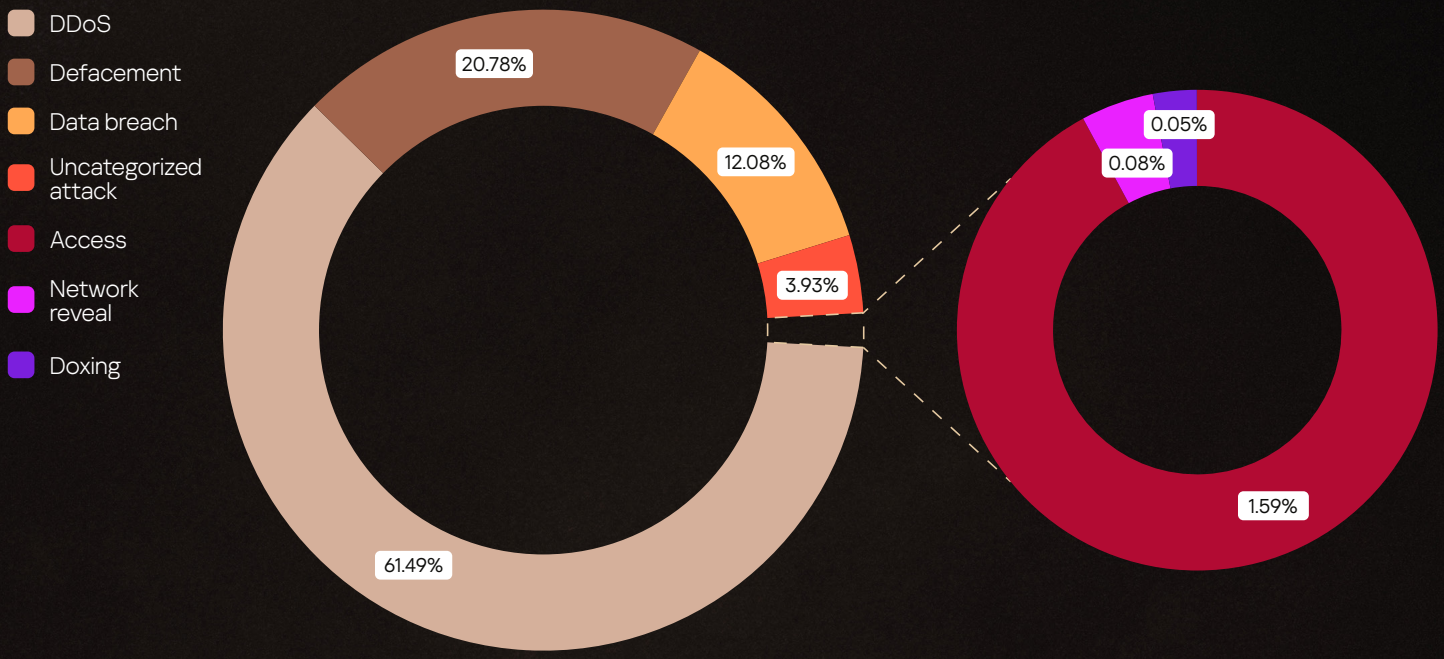
Reports on completed attacks are the most common hashtagged content, accounting for 59% of all hacktivist messages with hashtags.

Fig. 13 | Distribution of hacktivist message categories in 2025



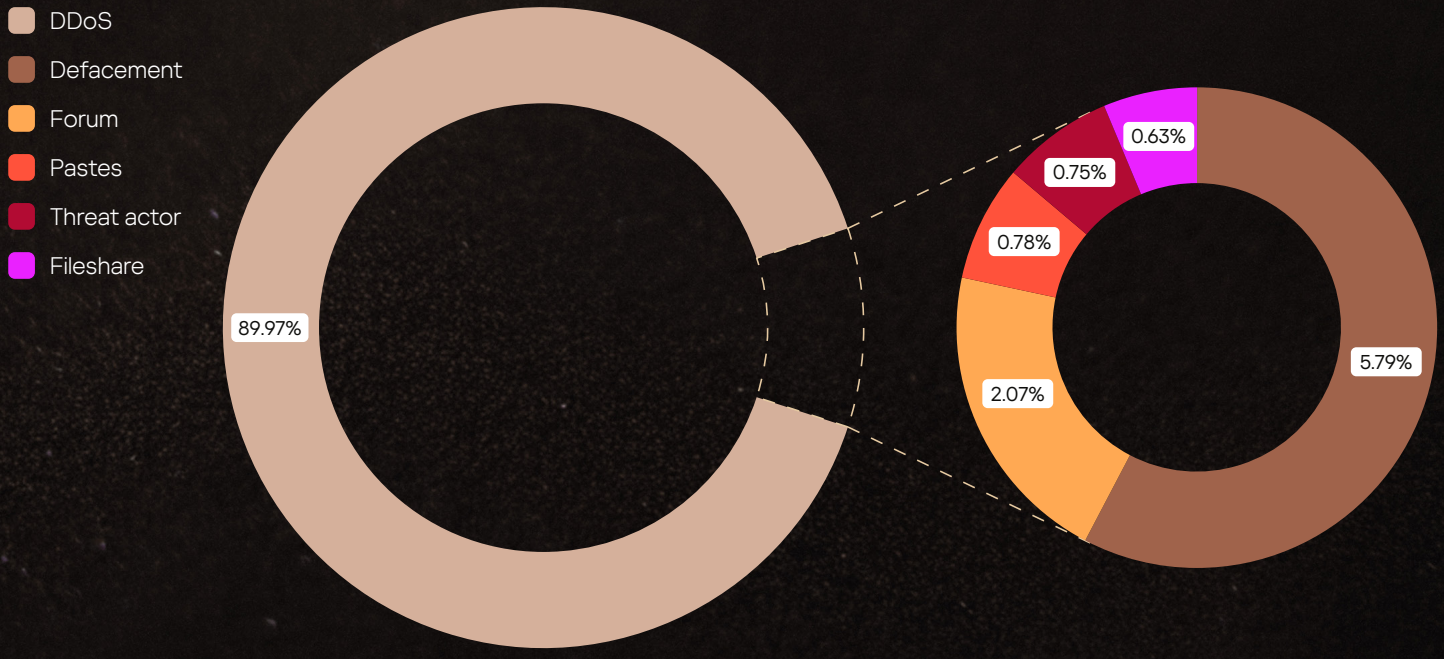
Within the “Completed attacks” category, 61% of messages relate to DDoS attacks.

Fig. 14 | Distribution of categories of completed hacktivist attack messages in 2025



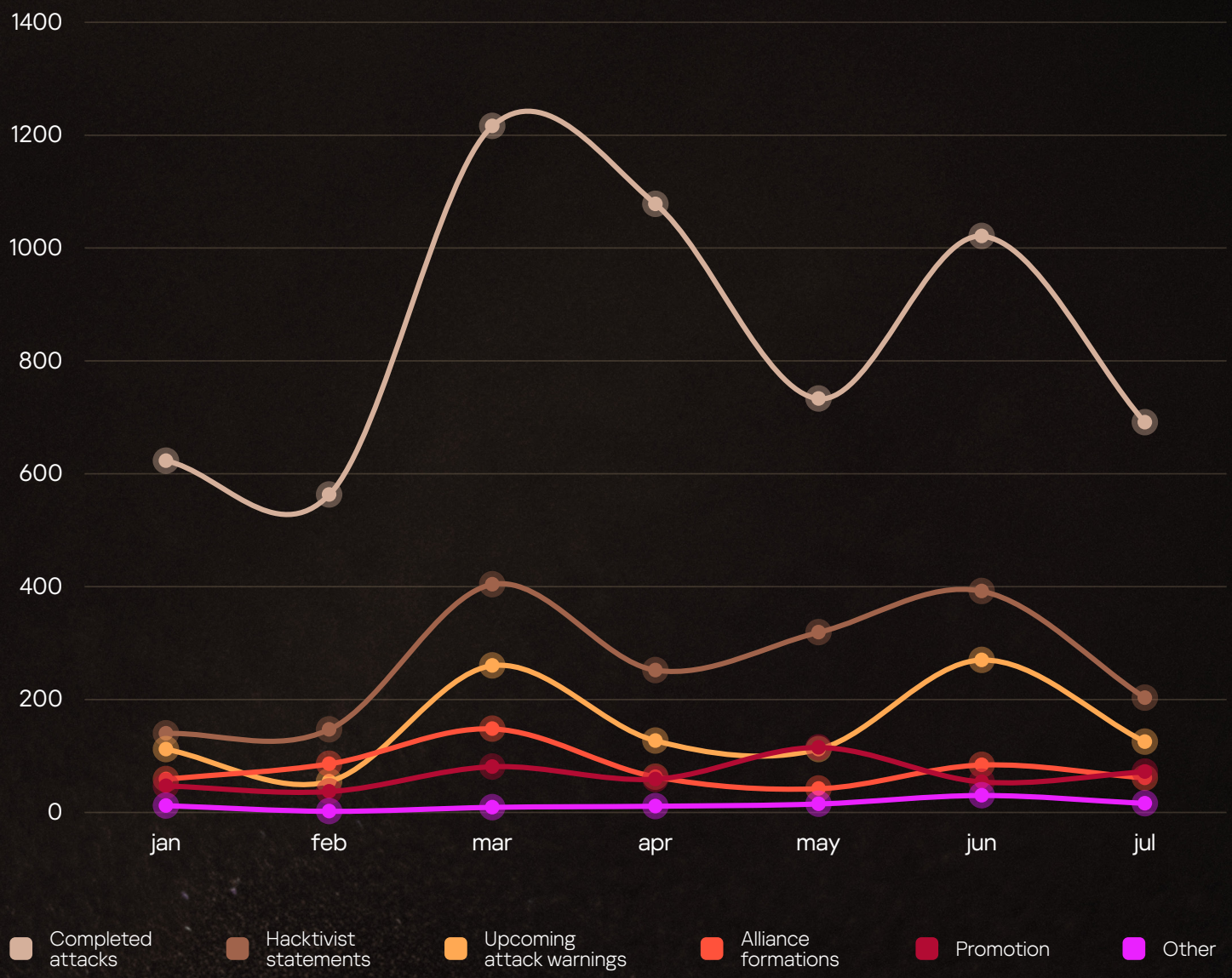
Analysis of external links further supports this trend: 90% of outbound links used for malicious purposes in hacktivist messages point to third-party resources that confirm DDoS outcomes (e.g. website downtime reports via check-host or similar tools).

Fig. 15 | Distribution of resources used for malicious purposes in 2025



The gap between DDoS-related posts (61%) and DDoS-related links (90%) shows that individual posts often cover multiple DDoS incidents. This makes DDoS not only the most common, but also the most heavily verified and reported tactic in the hacktivist toolkit.

Fig. 16 | Distribution of context of hashtagged messages in 2025



Insights

Despite periodic spikes in threat messages, there was no corresponding increase in reports of real cyberattacks. The volume of threats alone cannot predict future attack levels.

However, timing matters. When hacktivists issue threats, they usually refer to operations planned for the near future (often within the same week or month). This makes early detection of such warnings valuable for proactive defense. The earlier a business identifies a potential threat, the more time it has to patch vulnerabilities, apply DDoS protection measures, alert stakeholders, and activate mitigation measures.

Key conclusions

Targets are global:

Hacktivist activity is not limited to targets in the MENA region

Hashtag spikes track real-world events:

Activity often follows geopolitical developments, showing how hacktivists mobilize and draw attention during crises and times of increased geopolitical tensions

Telegram dominates communications:

88% of social media links in hashtagged messages point to Telegram

DDoS attacks continue to dominate the hacktivist landscape:

- **61%** of all attack reports involve DDoS
- **90%** of external links (excluding those to victim resources) in posts confirm website downtime
- A single post often documents multiple DDoS incidents

Hashtags are strategic tools, not just labels:

They serve as group identifiers, campaign markers, alliance signals, calls to action and political slogans

Most hashtags are short-lived:

Their average lifespan is about 2 months, unless amplified by alliances

A proactive, multi-layered defense is required to counter hacktivism

Do not underestimate hacktivist threats

Even if your business is outside the META region, you can still be a target.

Recomendations

Prioritize rapid threat detection and incident response

Treat hacktivist threats as short-term indicators; expect action within days — not months. Establish continuous monitoring, rapid threat discovery and resilient incident response capability, and layer in scalable DDoS mitigation.

- Kaspersky Next XDR Expert
- Kaspersky Managed Detection and Response
- Kaspersky Incident Response
- Kaspersky DDoS Protection

Continuously monitor the dark web and maintain up-to-date TTP insights

Use automated, real-time monitoring of the surface and dark web, apply cross-channel analysis, and issue early-warning alerts to equip teams with up-to-date insight into attacker TTPs.

- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Intelligence

Build workforce resilience

Strengthen resistance to phishing, social engineering, and hacktivist propaganda

- Kaspersky Security Awareness

Why Kaspersky?

Technology leadership based on world-class expertise

Unmatched human and AI expertise, driving innovation

Global presence and unique sources

Transparent and independently recognized

Active industry contributor

Kaspersky Digital Footprint Intelligence

Learn more

Powered by Security Services

www.kaspersky.com

#kaspersky
#bringonthefuture